ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ
INFORMATION TECHNOLOGY, COMPUTER SCIENCE, AND MANAGEMENT



УДК 004.89 10.23947/1992-5980-2017-17-4-116-121

Имитационное моделирование зависимости информационной безопасности организации от области деятельности*

О. Л. Цветкова[1], С. А. Заслонов[2]**
[1,2]Донской государственный технический университет, г. Ростов-на-Дону, Российская Федерация

Simulation modeling of organization's infosecurity dependence on field of activity ***

O. L. Tsvetkova[1], S. A. Zaslonov[2]**
[1,2] Don State Technical University, Rostov-on-Don, Russian Federation

Введение. Сформулировано решение задачи повышения эффективности системы защиты информации на предприятии путем своевременного выявления существенных факторов, влияющих на уровень информационной безопасности. Целью работы является разработка имитационной модели, отражающей влияние различных факторов, обусловленных показателями перспективности выбранной области деятельности организации, на эффективность функционирования системы защиты информации.
Материалы и методы. Имитационная модель реализована с использованием техники системной динамики в виде потоковой диаграммы. В качестве исходных данных предложено использовать обобщенные экспертные оценки перспективности направления деятельности. В модели применяются три системных уровня, которые определяют переменные состояния системы: степень эффективности системы защиты информации, бюджет организации на средства защиты информации и оценка качеств потенциальных нарушителей информационной безопасности. Также вводятся дополнительные параметры и переменные разрабатываемой модели: ценность информации, обрабатываемой в организации; оценка количества инцидентов информационной безопасности; текущие затраты на систему защиты информации; постоянный бюджет на систему защиты информации.
Результаты исследования. В качестве среды имитационного моделирования был выбран пакет *Vensim*. Анализ результатов моделирования показал, что характеристики области деятельности и качество информации, циркулирующей в информационной системе предприятия, напрямую определяют интерес со стороны потенциальных нарушителей, что приводит к необходимости четкого планирования и корректировки затрат на систему защиты информации. Таким образом, продемонстрирована возможность практического использования разработанной модели для оценки уровня информационной безопасности предприятий, осуществляющих свою деятельность в любой области. Отмечена необходимость привлечения экспертов с целью формирования оценок показателей перспективности возможных областей деятельности конкретной организации,

Introduction. The solution to the problem of efficiency improvement of the infosecurity system at the enterprise through early recognition of the essential factors affecting the level of information safety is defined. The work objective is to develop a simulation model that represents the effect of various factors caused by indicators of prospects of the selected area of the organization activity on the data protection system performance effect.
Materials and Methods. The simulation model is implemented using the system dynamics equipment in the form of the streaming graph. It is proposed to use generalized expert assessments of the activity prospects as source data. The model applies three system levels that determine system state variables: level of efficiency of the data protection system, organization's budget on information security tools, and the quality assessment of the potential infringers of cybersecurity. Besides, additional parameters and variables of the developed model are introduced: value of the information processed in the organization; estimated number of security incidents; current costs for the information security system; and continuous budget on the cybersecurity system.
Research Results. Vensim package is selected as a simulation environment. The modeling outcome analysis has shown that characteristics of the activity field and quality of the information circulating in the information system of the organization directly determine the interest of potential intruders that leads to the need for careful budgeting and adjustment of costs for the information security system. Thus, the implementability of the developed model for the assessment of the information safety level of the enterprises which operate in any area is shown. However, the involvement of experts in order to form assessments of indicators of prospects for eligible activity sectors of a particular organization and to conduct

* Работа выполнена в рамках инициативной НИР.
** E-mail: olga_cvetkova@mail.ru, yamdfst@mail.ru
*** The research is done within the frame of the independent R&D.

проведения аудита ее системы защиты.

Обсуждение и заключения. Реализация имитаций разработанной модели с различными начальными условиями и входными данными позволила определить динамику изменения информационной безопасности, обеспечить своевременное и эффективное развитие системы защиты, поддержку принятия решений специалистами службы безопасности при планировании расходов на защиту информации и изменений политики безопасности организации.

an audit on its protection system is required.

Discussion and Conclusions. Implementation of the developed model simulations under various entry conditions and entrance data allows for the definition of the dynamic patterns of IT security, and support for decision-making by security specialists when planning expenses on information security and changes in organization security policy.

Ключевые слова: имитационное моделирование, системная динамика, потоковая диаграмма, причинно-следственная диаграмма, информационная безопасность, система защиты информации, оценка эффективности системы защиты информации, аудит системы защиты информации, потенциальный нарушитель информационной безопасности, конфиденциальная информация.

Keywords: simulation modeling, system dynamics, streaming graph, cause-effect diagram, cybersecurity, information security system, effectiveness evaluation of information security system, audit of data protection system, potential infringer of information security, private data.

Образец для цитирования: Цветкова, О. Л. Имитационное моделирование зависимости информационной безопасности организации от области деятельности / О. Л. Цветкова, С. А. Заслонов // Вестник Дон. гос. техн. ун-та. — 2017. — Т. 17, № 4. — С. 116–121.

For citation: O.L. Tsvetkova, S.A. Zaslonov. Simulation modeling of organization's infosecurity dependence on field of activity. Vestnik of DSTU, 2017, vol. 17, no.4, pp. 116–121.

Введение. Задача защиты конфиденциальной информации является очень важной, от эффективности и своевременности ее решения во многом зависит процесс функционирования предприятия, наличие прибыли, конкурентоспособность, репутация. Для предприятий особенно важным является защита коммерческой информации от кражи и несанкционированного доступа. Заметим, что утечка информации может произойти непреднамеренно, вследствие небрежности сотрудников, или преднамеренно, например, по заказу конкурентов.

Появление новых угроз информационной безопасности (ИБ) и средств защиты приводят к необходимости модификации и развития системы защиты. Однако, как отмечено в [1], внедрение инновационных методов в сферу ИБ может сопровождаться определенными проблемами. Для оценки эффективности принимаемых решений и достигнутого уровня ИБ используются различные подходы [2, 3]. Одним из актуальных направлений подобных исследований, которое имеет как теоретическую, так и практическую ценность, является анализ процессов взаимодействия систем защиты информации с окружающей средой, выявление факторов, оказывающих существенное влияние на эффективность защиты.

В настоящей работе выполняется построение имитационной модели, описывающей динамику влияния показателей перспективности выбранной области деятельности организации на систему защиты информации, целями создания которой является изучение процессов, протекающих в системе, а также обеспечение поддержки принятия решений при управлении системой защиты информации.

Использование техники имитационного моделирования для решения поставленных задач обусловлено тем, что исследуемые процессы воздействия различных факторов на систему защиты информации характеризуются наличием причинно-следственных связей, стохастических переменных, влиянием последствий. Подобные задачи исследования систем защиты информации с помощью имитационного моделирования рассматривались в ряде научных работ [4, 5]. Имитационное моделирование является популярным видом моделирования, используется в научных и прикладных областях для построения моделей разнообразных систем [6–9].

Разработка имитационной модели. Существует три основных подхода к имитационному моделированию: агентное, дискретно-событийное моделирование и системная динамика [10]. Эти подходы отличаются уровнем абстракции, точкой зрения на специфические процессы, протекающие в системе, на взаимосвязи между элементами, на правила и законы, определяющие динамику развития исследуемой системы.

Для решения поставленных задач предлагается использовать системную динамику, поскольку этот вид имитационного моделирования способствует наилучшему пониманию специфических особенностей процессов,

протекающих в системе, позволяет выявить причинно-следственные связи между объектами [11]. Методология системной динамики, предложенная Дж. Форрестером, основана на использовании потоковых диаграмм, обеспечивающих представление системы в виде структуры с обратными связями, и отображающих влияние одних параметров на другие [12].

Основными составляющими потоковых диаграмм являются: накопители (системные уровни); потоки (системные темпы); правила (обратные связи). Системные уровни представляют состояние системы. Системные темпы реализуют динамику системы, изменяют значения системных уровней и характеризуют скорость этого изменения, причем проводится разделение на входящие и выходящие потоки. Обратные связи определяют взаимное влияние элементов системы.

Для системных уровней составляется система дифференциальных уравнений по Дж. Форрестеру [12]:

$$\frac{d\bar{x}}{dt} = f(\bar{x}, \bar{a}) = \bar{x}^{+} - \bar{x}^{-},$$

где $f(\bar{x}, \bar{a})$ — вектор-функция, зависящая от переменных $\bar{x}$ и параметров $\bar{a}$ модели; $\bar{x}^{+}$, $\bar{x}^{-}$ — положительный и отрицательный темпы изменения системных уровней $\bar{x}$, содержащие факторы роста и убывания $\bar{x}$.

Исходными данными для имитационной модели являются экспертные оценки показателей перспективности области деятельности организации, выбор которой влияет на качества циркулирующей в организации информации, на прибыль и на заинтересованность со стороны потенциальных нарушителей.

В качестве системных уровней (накопителей), которые определяют переменные состояния системы, в модели предлагается использовать:

- степень эффективности системы защиты информации (Q);
- бюджет организации на средства защиты информации (СЗИ) — количество денежных средств, выделяемых на модификацию и содержание системы защиты информации (K);
- оценку качеств потенциальных нарушителей ИБ — обобщенный показатель, характеризующий количество потенциальных нарушителей, их заинтересованность, материальную и техническую оснащенность, профессиональные навыки (N).

Таким образом, на уровень ИБ будет влиять три величины, для которых в соответствии с [12] составляются дифференциальные уравнения:

$$\begin{cases} dQ/dt = Q^{+} - Q, \\ dK/dt = K^{+} - K, \\ dN/dt = N^{+} - N, \end{cases}$$

где Q^{+}, Q — темпы увеличения и снижения эффективности системы защиты информации соответственно; K^{+}, K — скорости увеличения и уменьшения капитала организации соответственно; N^{+}, N — темпы увеличения и снижения умений, возможностей и заинтересованности потенциальных нарушителей ИБ.

Дополнительные параметры и переменные разрабатываемой имитационной модели:

- обобщенная оценка показателей перспективности области деятельности организации. Используется в качестве входной переменной, получаемой на основе экспертных оценок, учитывающих актуальность, прибыльность области деятельности, а также оценку уровня заинтересованности потенциальных нарушителей (конкурентов, нелояльных сотрудников, хакеров) в информации, циркулирующей в организации;
- ценность информации, обрабатываемой в организации, прямо пропорциональная обобщенной оценке показателей перспективности области деятельности организации;
- оценка количества инцидентов ИБ — показатель, зависящий от активности потенциальных нарушителей;
- текущие затраты на СЗИ, зависящие от оценки количества возникающих инцидентов ИБ;
- постоянный бюджет на СЗИ — константа, определяемая на основе аналитических прогнозов изменения условий функционирования организации и требований к защите информации.

Разработанная потоковая диаграмма представлена на рис. 1.

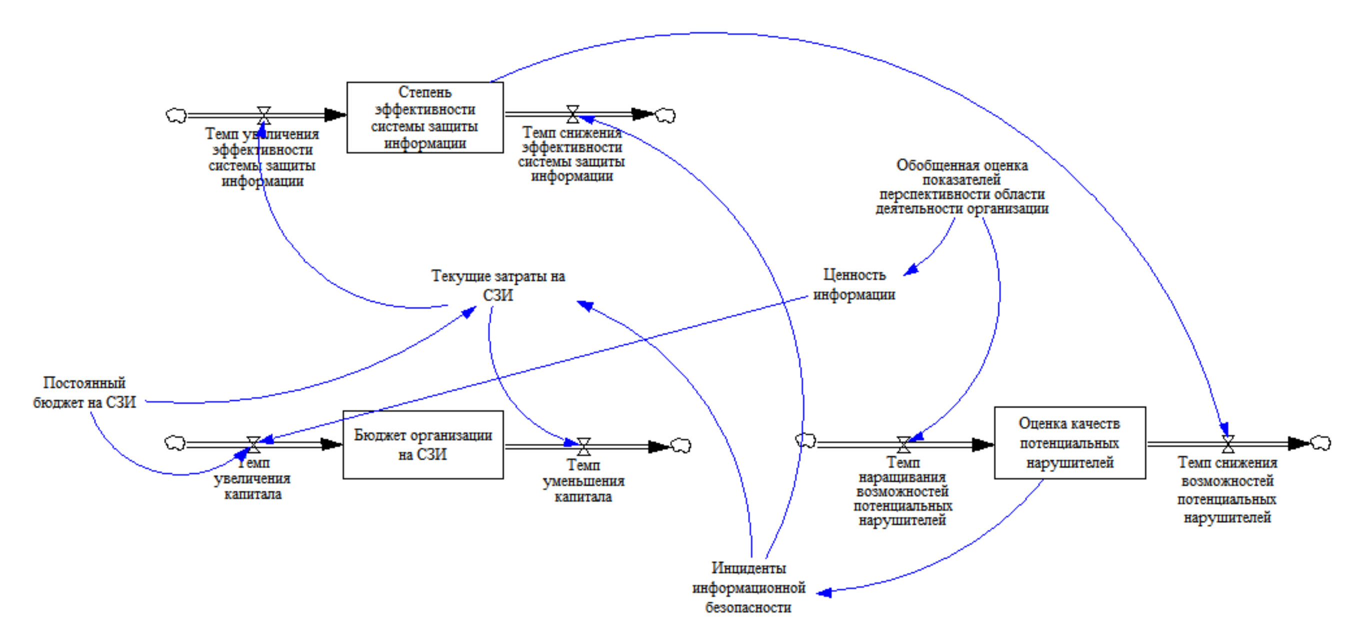
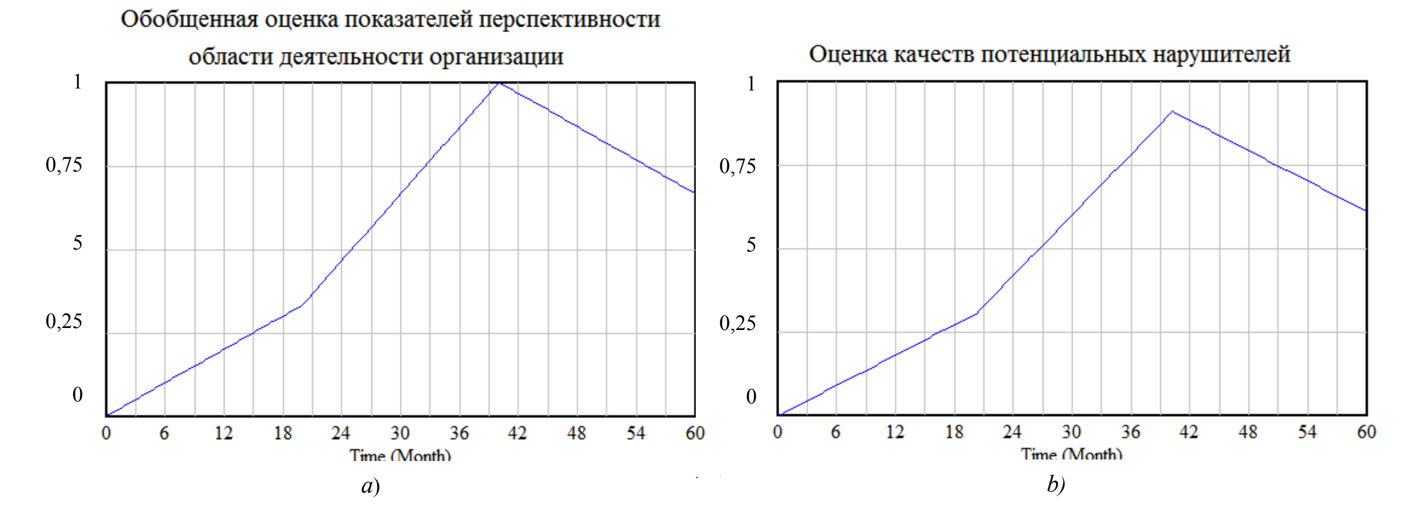


Рис. 1. Потоковая диаграмма

Fig. 1. Streaming graph

Проведение имитаций и анализ результатов. В качестве среды имитационного моделирования для проведения компьютерных имитаций был выбран пакет *Vensim*, разработанный фирмой *Ventana Systems, Inc*. Пакет предназначен для визуализации моделей системной динамики, представляемых в виде причинно-следственных (потоковых) диаграмм, состоящих из накопителей и потоков. Такие диаграммы отображают связи межу элементами системы, их взаимодействие и влияние друг на друга. Результаты имитационного моделирования представлены на рис. 2.

Разработанная модель может быть применена для оценки уровня ИБ предприятий, осуществляющих свою деятельность в любой области. Однако для этого необходимо привлечение экспертов с целью формирования оценок показателей перспективности возможных областей деятельности конкретной организации, проведения аудита ее системы защиты.



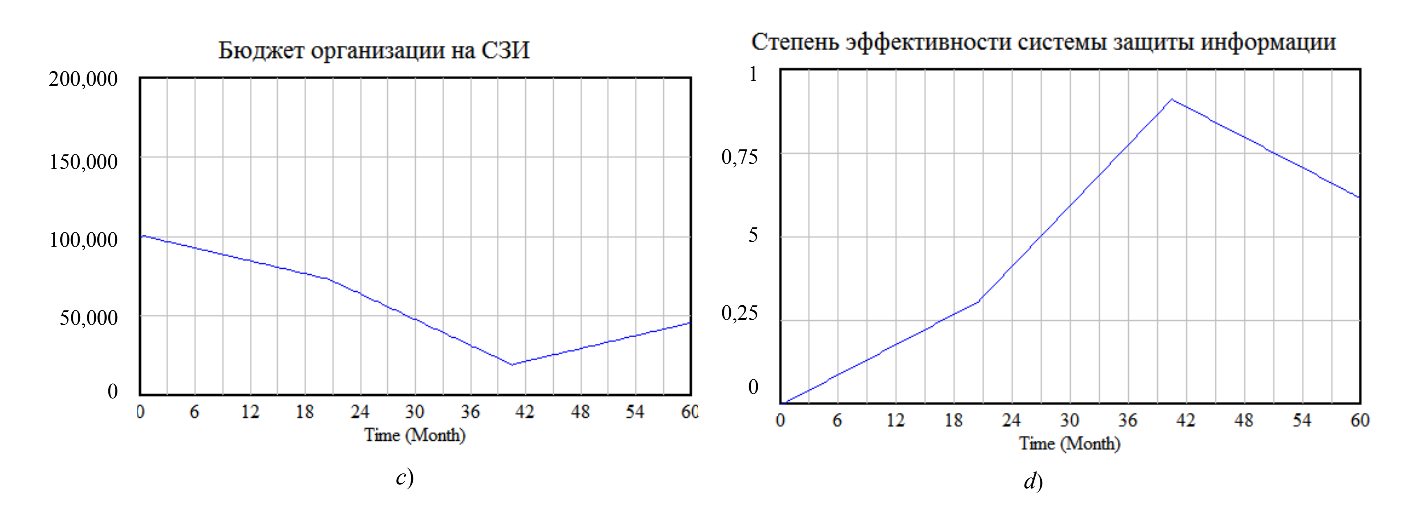


Рис. 2. Результаты имитационного моделирования

Fig. 2. Simulation modeling outcomes

Заключение. Использование результатов имитационного моделирования обеспечивает поддержку принятия решений специалистами службы безопасности при планировании расходов на защиту информации, внесения изменений в политику безопасности организации, позволяет своевременно и эффективно развивать систему защиты.

Библиографический список

1. Айдинян, А. Р. Проблемы внедрения инновационных методов в сферу информационной безопасности / А. Р. Айдинян // Инновационные исследования : проблемы внедрения результатов и направления развития: сб. ст. междунар. науч.-практ. конф. — Омск : МЦИИ «Омега сайнс», 2016. — Ч. 2. — С. 9–11.

2. Черняков, П. В. Двухуровневая система оценки средств защиты компьютерной информации от утечек / П. В. Черняков, А. Р. Айдинян, О. Л. Цветкова // Инновационная наука. — 2016. — № 3–3. — С. 140–144.

3. Цветкова, О. Л. Интеллектуальная система оценки информационной безопасности предприятия от внутренних угроз / О. Л. Цветкова, А. Р. Айдинян // Вестник компьютерных и информационных технологий. — 2014. — № 8 (122). — С. 48–53.

4. Иванов, Е. В. Методы имитационного моделирования подсистемы безопасности процессингового центра / Е. В. Иванов, А. И. Иванова // Вестник российского нового ун-та. — 2010. — № 3. — С. 67–73.

5. Sarriegi, J.M., Santos, J., Torres, J.M., Imizcoz, D., Plandolit, A.L. Modeling Security Management of Information Systems: Analysis of an Ongoing Practical Case // Conference Proceedings: the 24th International Conference of the System Dynamics Society. — Nijmegen, the Netherlands, 2006.

6. Лукьянов, В. Ф. Имитационное моделирование многоочагового разрушения с учетом неоднородного распределения номинальных напряжений / В. Ф. Лукьянов, С. С. Ассауленко // Вестник Дон. гос. техн. ун-та. — 2015. — № 4 (83). — С. 31–36.

7. Бутов, А. А. Стохастическое имитационное моделирование механизмов укорочения теломер клеток в процессах старения и развития патологических отклонений / А. А. Бутов, М. А. Карев, С. А. Хрусталев // Вестник Дон. гос. техн. ун-та. — 2014. — Т. 14. — № 1 (76). — С. 98–109.

8. Городнова, Н. В. Имитационное моделирование устойчивости деятельности государственно-частного партнерства в строительстве / Н. В. Городнова // Вестник Дон. гос. техн. ун-та. — 2012. — № 2 (63), вып. 1. — С. 73–80.

9. Кантор, О. Г. Построение моделей системной динамики в условиях ограниченной экспертной информации / О. Г. Кантор, С. И. Спивак // Информатика и ее применение. — 2014. — Т. 8, № 2. — С. 111–121.

10. Борщев, А. В. Практическое агентное моделирование и его место в арсенале аналитика / А. В. Борщев // Имитационное моделирование. Теория и практика : сб. докл. II всеросс. науч.-практ. конф. ИММОД–2005. — Санкт-Петербург : ЦНИИТС, 2005. — Т. 1. — С. 11–24.

11. Wolstenholme, E. F. System enquiry : a system dynamic approach. — Chichester, England : John Wiley and Sons, 1990. — 238 p.

12. Forrester, J. World dynamics. — Wright-Allen Press, 1971. — 144 p.

References

1. Aydinyan, A.R. Problemy vnedreniya innovatsionnykh metodov v sferu informatsionnoy bezopasnosti. [Problems of introduction of innovative methods in the information security area.] Innovatsionnye issledovaniya: problemy vnedreniya rezul'tatov i napravleniya razvitiya: sb. st. mezhdunar. nauch.-prakt. konf. [Innovative research: problems of results implementation and

tendencies of development: Proc. Int. Sci.-Pract. Conf.] Omsk: MTsII "Omega Science", 2016, part 2, pp. 9–11 (in Russian).

2. Chernyakov, P.V., Aydinyan, A.R., Tsvetkova, O.L. Dvukhurovnevaya sistema otsenki sredstv zashchity komp'yuternoy informatsii ot utechek. [A two-level system for assessing means of leak protection of computer information.] Innovatsionnaya nauka, 2016, no. 3–3, pp. 140–144 (in Russian).

3. Tsvetkova, O.L., Aydinyan, A.R. Intellektual'naya sistema otsenki informatsionnoy bezopasnosti predpriyatiya ot vnutrennikh ugroz. [Intelligent system evaluation information security of the enterprise from internal threats.] Herald of Computer and Information Technologies, 2014, no. 8 (122), pp. 48–53 (in Russian).

4. Ivanov, E.V., Ivanova, A.I. Metody imitatsionnogo modelirovaniya podsistemy bezopasnosti protsessingovogo tsentra. [Imitation modeling methods of security subsystems of a processing center.] Vestnik of Russian New University, 2010, no. 3, pp. 67–73 (in Russian).

5. Sarriegi, J.M., Santos, J., Torres, J.M., Imizcoz, D., Plandolit, A.L. Modeling Security Management of Information Systems: Analysis of an Ongoing Practical Case. Conference Proceedings: the 24th International Conference of the System Dynamics Society. Nijmegen, the Netherlands, 2006.

6. Lukyanov, V.F., Assaulenko, S.S. Imitatsionnoe modelirovanie mnogoochagovogo razrusheniya s uchetom neodnorodnogo raspredeleniya nominal'nykh napryazheniy. [Simulation of multicentric destruction with regard for inhomogeneous distribution of rated voltage.] Vestnik of DSTU, 2015, no. 4 (83), pp. 31–36 (in Russian).

7. Butov, A.A., Karev, M.A., Khrustalev, S.A. Stokhasticheskoe imitatsionnoe modelirovanie mekhanizmov ukorocheniya telomer kletok v protsessakh stareniya i razvitiya patologicheskikh otkloneniy. [Stochastic simulation modeling of cell telomere shortening mechanisms in ageing and disturbance development processes.] Vestnik of DSTU, 2014, vol. 14, no. 1 (76), pp. 98–109 (in Russian).

8. Gorodnova, N.V. Imitatsionnoe modelirovanie ustoychivosti deyatel'nosti gosudarstvenno-chastnogo partnerstva v stroitel'stve. [Simulation modeling of work stability of state-private partnership in construction.] Vestnik of DSTU, 2012, no. 2 (63), iss. 1, pp. 73–80 (in Russian).

9. Kantor, O.G., Spivak, S.I. Postroenie modeley sistemnoy dinamiki v usloviyakh ogranichennoy ekspertnoy informatsii. [Construction of system dynamics models in conditions of limited expert information.] Informatics and Applications, 2014, vol. 8, no. 2, pp. 111–121 (in Russian).

10. Borshchev, A.V. Prakticheskoe agentnoe modelirovanie i ego mesto v arsenale analitika. [Practical agent modeling and its place in the analyst's toolkit.] Imitatsionnoe modelirovanie. Teoriya i praktika: sb. dokl. II vseross. nauch.-prakt. konf. IMMOD–2005. [Simulation modeling. Theory and practice: Proc. II All-Russian Sci.-Pract. Conf. IMMOD–2005.] St. Petersburg: TsNIITS, 2005, vol. 1, pp. 11–24 (in Russian).

11. Wolstenholme, E. F. System enquiry: a system dynamic approach. Chichester, England: John Wiley and Sons, 1990, 238 p.

12. Forrester, J. World dynamics. Wright-Allen Press, 1971, 144 p.

Поступила в редакцию 22.06.2017
Сдана в редакцию 23.06.2017
Запланирована в номер 15.09.2017

Received 22.06.2017
Submitted 23.06.2017
Scheduled in the issue 15.09.2017

Об авторах:

Цветкова Ольга Леонидовна,
доцент кафедры «Вычислительные системы и информационная безопасность» Донского государственного технического университета (ДГТУ) (РФ, 344000, г. Ростов-на-Дону, пл. Гагарина,1), кандидат технических наук, доцент,
ORCID: http://orcid.org/0000-0003-4071-6313
olga_cvetkova@mail.ru

Заслонов Сергей Андреевич,
студент кафедры «Вычислительные системы и информационная безопасность» Донского государственного тех-нического университета (ДГТУ) (РФ, 344000, г. Ростов-на-Дону, пл. Гагарина,1),
ORCID: http://orcid.org/0000-0002-5207-770X
yamdfst@mail.ru

Authors:

Tsvetkova, Olga L.,
associate professor of the Computer Systems and Information Security Department, Don State Technical University (RF, 344000, Rostov-on-Don, Gagarin Square, 1), Cand.Sci. (Eng.), associate professor,
ORCID: http://orcid.org/0000-0003-4071-6313
olga_cvetkova@mail.ru

Zaslonov, Sergey A.,
student of the Computer Systems and Information Security Department, Don State Technical University (RF, 344000, Rostov-on-Don, Gagarin Square, 1),
ORCID: http://orcid.org/0000-0002-5207-770X
yamdfst@mail.ru